

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH
WALKER.JEFF@ME.COM THAT IS STORED AT THE
PREMISES CONTROLLED BY APPLE, INC.

Case No.

3:17mj 473

FILED
RICHARD W. NAGEL
CLERK OF COURT
2017 OCT 11 PM 4:26
U.S. DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
DAYTON

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

26 U.S.C. 7201

Offense Description

Attempt to evade or defeat tax

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

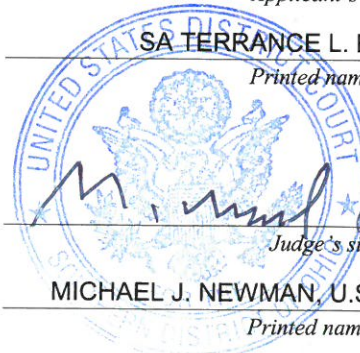

Date: 10/11/17

City and state: DAYTON, OHIO


 Applicant's signature

SA TERRANCE L. BROWN, IRS-CID

Printed name and title



 Judge's signature

MICHAEL J. NEWMAN, U.S. MAGISTRATE JUDGE

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION**

IN THE MATTER OF THE SEARCH OF : Case No.
INFORMATION ASSOCIATED WITH :
WALKER.JEFF@ME.COM :
THAT IS STORED AT PREMISES : Filed Under Seal
CONTROLLED BY APPLE, INC. :

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Terrance Brown, a Special Agent with the Internal Revenue Service, Criminal Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. an e-mail provider headquartered at 1 Infinite Loop, M/S 169-5CLP, Cupertino, California 95014. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703 (c)(1)(A) to require Apple, Inc. to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am and have been a Special Agent with the Internal Revenue Service, Criminal Investigation since 2005. I received training in investigating financial, tax, and money laundering crimes at the Federal Law Enforcement Training Center. I have also attended seminars and had additional training on tax crimes and other financial schemes. My primary duty is to investigate criminal violations of Title 26 U.S.C. (Internal Revenue Laws). During my

time as a Special Agent, I have written multiple search and seizure warrant affidavits and investigated schemes involving tax evasion, money laundering, and other fraudulent activities.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 26 U.S.C. § 7201 have been committed by Jeff Walker. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. §2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

PROBABLE CAUSE

5. On or about October 6, 2016, I spoke with a Confidential Informant (“CI-1”),¹ who stated, in substance and in part, the following:

- a. In or about August 2015, Jeff Walker solicited offers to sell his automobile dealership. Walker was attempting to sell the dealership to multiple potential purchasers. Walker’s automobile dealership was operated under the name Walker Chrysler Jeep Dodge Ram and was located in Dayton, Ohio.

¹The information provided by CI-1 was deemed reliable because, as noted below, it was corroborated by IRS records. CI-1, who is not a government employee, would not have reason to know what information has been provided to the IRS on behalf of Walker or Walker’s dealership. CI-1’s information is further corroborated by the timing of the sale soliciting email (August 2015) and the actual sale of Walker’s dealership (November 2015).

- b. During the solicitation to sell the dealership, Walker sent an email message (the “Email”) from the email account walker.jeff@me.com (the “Subject Account”), which was received by CI-1.
- c. Attached to the Email was a spreadsheet that appeared to be a summary of expenses of the dealership for the years 2011-2014, which the Email explained as “a comprehensive spreadsheet documenting all areas of profitability and non-dealership related Owner/Owner family expenses considered add-backs to profit.” The Email noted, “[T]hese are exactly the same numbers the other dealer is using.” The identity of the “other dealer” was not known to CI-1, but presumably the other dealer was also interested in purchasing Walker Chrysler Jeep Dodge Ram.
- d. Some of those headings on the spreadsheet were “Wages,” “Personal Family,” “RV,” “NCR CC,” “Shell/Speedway,” and “Owner Expenses” (listed twice).
- e. Under the heading “Wages”: “Includes all monies paid to both owners and the owner’s children (none of which work at the store).”
- f. Under the heading “Personal Family”: “Both owners family have full family LA Fitness memberships. This category includes the additional insurance the store paid for all the non-owner drivers in the 2 families (10 folks total). The owners were in control of 14 vehicles at all times (6 for my partner’s family and 8 for my family).”
- g. Under the heading “RV”: “I bought a motorhome and am the only person to ever use it. It has never been used by any employee or customer. I added back the interest from payments, storage fees and general expenses from maintaining it and a driver.”

- h. Under the heading "Owner Expenses": "I used very liberally my 2 company credit cards for considerable person items. Things like over 50k in wine, 1000's for sports tickets, consumer goods purchases, household goods, fuel for boats, etc. Nothing in this list had anything to do with the dealership."
 - i. Under the heading "NCR CC": "Both owners had their annual dues and monthly expenses at NCR CC paid for by the company. In 2011-2012, I did a car trade with the club whereby both owners dues were traded out in exchange for a vehicle."
 - j. Under the heading "Shell/Speedway": "Fuel used by owners gas cards."
 - k. Under the heading "Owner Expenses": "This credit card is AMEX (the other one was Visa) of more personal expenses I charged to the store for years."
6. The information I have reviewed that was provided by CI-1 indicates that there were personal diversions from the dealership during tax years 2011-2014 totaling at least \$500,000.
7. I have reviewed an article in the Dayton Daily News dated November 10, 2015, which confirmed the dealership was sold on November 10, 2015.
8. I have reviewed IRS records, and from that review, I have learned, among other things, that (1) children of Jeff Walker received Forms W-2 from the dealership; and (2) Jeff Walker was a 51% owner of Walker Chrysler Jeep Dodge Ram during 2011-2015.
9. Based on my training and experience, I know that individuals who pay personal expenses through businesses they control typically do not include such expenses as income on their personal income tax returns. From the above paragraphs, it seems likely that Walker paid personal expenses through his business. It is also likely that Walker did not include the personal expenses paid through the business as personal income on his tax returns.

10. Based on my training and experience, one mechanism used to evade income tax is to pay wages to individuals as “employees” who were not in fact employees. Based on my review of the Email and IRS records, it appears that Walker is attempting to evade income taxes.

11. Based on my training and experience, I know that individuals involved in criminal activity, and individuals in general, do not always dispose of email messages in their ‘sent’ or their ‘deleted’ email folders. Even if individuals do dispose of email messages in their ‘sent’ and ‘deleted’ email folders, in today’s world of cloud computing, rarely do individuals ever completely dispose of messages. Based on my training and experience, I believe it is likely that messages relating to the dealership’s potential and eventual sale, and evidence of tax evasion, are still in the Subject Account.

12. On or about September 28, 2017, I served a preservation request to Apple for the Subject Account. In general, an email that is sent to an Apple subscriber is stored in the subscriber’s “mail box” on Apple’s servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Apple’s servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Apple’s servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

13. In my training and experience, I have learned that Apple provides a variety of on-line services, including electronic mail (“email”) access, to the public. Apple allows subscribers to obtain email accounts at the domain name me.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Apple. During the registration process, Apple asks subscribers to provide basic personal information. Therefore, the computers of Apple are likely to contain stored electronic communications (including retrieved and unretrieved email for Apple subscribers) and information concerning subscribers and their use of Apple services, such as account access information, email transaction information, and account

application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

15. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account. ✍

16. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as

technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. This application seeks a warrant to search all responsive records and information under the control of Apple, a provider subject to the jurisdiction of this court, regardless of where Apple has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Apple's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.¹

18. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct

¹ It is possible that Apple stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2d Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this

warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Apple. However, I am mindful of the Court's previous decision that a request for information stored, held, or maintained outside of the United States is premature at this time because the location(s) where Apple stores, holds, or maintains the responsive information sought by the warrant is unknown at the present time. Accordingly, the government requests that the Court order, via Attachment B, that Apple disclose in writing to the government the physical location(s) where the responsive information is stored, held, and/or maintained, whether inside or outside of the United States.

under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

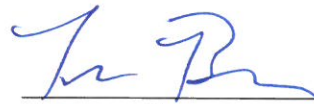
CONCLUSION

19. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Apple, who will then compile the requested records at a

time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

20. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

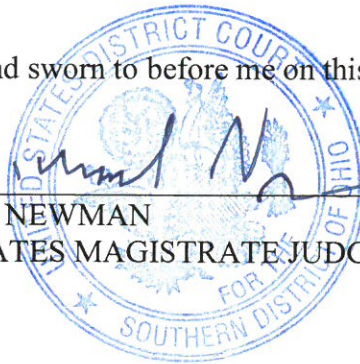


Terrance Brown
Special Agent, IRS-CID

Subscribed and sworn to before me on this 11th day of October, 2017



MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following e-mail addresses and accounts that are stored at premises controlled by Apple, Inc., within the Unites States and/or its territories, see In re Warrant, 829 F.3d 197 (2nd Cir. 2016), a company that accepts service of legal process at the address listed below:

| Address of Target E-mail Accounts | Electronic Mail Service Provider |
|-----------------------------------|--|
| walker.jeff@me.com | Apple, Inc. 1 Infinite Loop Cupertino, California 95014 subpoenas@apple.com |

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Apple, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider. The Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period of March 1, 2015 through November 17, 2015:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

II. Information to be seized by the government

All information described above that constitutes evidence tax evasion by Jeff Walker, and others, including information pertaining to the following matters:

- a. Any communications relating to the sale or potential sale of Walker Chrysler Jeep Dodge Ram or other businesses.
- b. Any communications relating to personal or business income taxes, expenses, or recordkeeping.
- c. Any records pertaining to the deletion or altering (or attempts to do so) of information in the email account.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple, Inc., and my official title is _____. I am a custodian of records for Apple, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple, Inc.; and
- c. such records were made by Apple, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature